REMARKS

Reconsideration and allowance of this application are respectfully requested. Claims 1-15 remain pending. By this communication, claims 3 and 4 are amended. Specifically, claims 3 and 4 have been rewritten in independent form.

Rejection Under 35 U.S.C. § 103

Claims 1-15 stand rejected under 35 U.S.C. §103(a) for alleged unpatentability over *Aura* (U.S. Patent No. 6,373,949) in view of *Labaton* (U.S. Patent Publication No. 2006-0005028). Applicant respectfully traverses this rejection.

Aura discloses a method for protecting transmission of a user identity to the user's home network in a data communications system. The method is implemented by using the algorithm presented in Figure 5 of *Aura*. The mobile station MS first generates, in phase 501, a random number RAND1. *Aura*, col. 4, lines 39-41 and Figure 5. In phase 502, the mobile station generates a cipher key Kd using a one-way hash function H4. *Id.*, col. 4, lines 45-47. For input data for the function, the random number RAND1 and a key Kh, which is specific to the home location register (HLR) of the user's network, are used. *Id.*, col. 4, lines 45-47. In phase 503, the mobile station encrypts its IMSI identity using the Kd key and IMSI identifier as input data for a cipher algorithm E, and sends its encrypted identity and the random number RAND1 to network VPLMN. *Id.*, col. 5, lines 9-12. The network receives the message. To transmit the subscriber's message to the correct home location register, the network must be able to determine the subscriber's HLR address from the message. *Id.*, col. 5, lines 13-16. To achieve this, it is preferable to use the E

algorithm as the cipher algorithm because it leaves the HLR-specified section of the identifier non-encrypted. *Id.*, col. 5, lines 16-18.

After determining the subscriber's home location register address from the message received, the network forwards the message containing the encrypted identifier data EIMSI and random number RAND1 to the home location register HLR. *Id.*, col. 5, lines 23-27. In phase 505, HLR computes the cipher key Kd by means of the key Kh known to it and the random number RAND1 received from the mobile station. *Id.*, col. 5, lines 33-35. In phase 506, HLR deciphers the subscriber identifier IMSI using the Kd key and the encrypted EIMSI identity provided by the mobile station. *Id.*, col. 5, lines 35-37.

As discussed above, in the method of *Aura*, the user's identity data is sent to the network using a cipher key common to a certain group of users and a random number which is sent to the network attached to the encrypted identity data. Specifically, *Aura* discloses dividing an user identifier into a first and second section such that the first section includes data necessary for identifying a user group, e.g. the HLR, and the second section identifies a user within the user group. A random input is generated at the user station, and the second section of the user's identifier is encrypted using the random input and a cipher key specific to each user group.

In regards to independent claims 1, 8, and 10, the Office acknowledges that *Aura* does not disclose using an asymmetrical algorithm. However, the Examiner asserts that *Labaton* discloses using an asymmetrical algorithm and that the combination would be obvious (*See* Office Action, pg. 3). Applicant respectfully disagrees.

Though *Labaton* teaches using an asymmetrical algorithm, the use of an asymmetrical algorithm in *Aura* would not work. *Aura* discloses encrypting the IMSI identifier using a cipher key ("the kd key"), and decrypting the identifier using the same kd key. Thus, the Office is incorrect in its assessment that two keys are being used, one for encrypting and the other for decrypting (*See* Office Action, pg. 3). The "kh key," in addition to the random number input, is merely being used to calculate the kd key. Thus, *Aura* actually teaches away from the use of an asymmetrical algorithm, because the same key must be generated at both the sending and receiving terminals. Accordingly, a person of ordinary skill in the art would not be motivated to combine Aura's method of encrypting/decrypting a subscriber identifier using an asymmetrical algorithm as taught by *Labaton*.

Therefore, *Aura* or *Labaton*, alone or in combination, cannot render independent claims 1, 3, 4, 8, and 10 obvious to one skilled in the art. Claims 2, 5-7, 9, 11-15, dependent from either independent claims 1, 8, or 10, are patentable at least for the reasons stated above with respect to these independent claims.

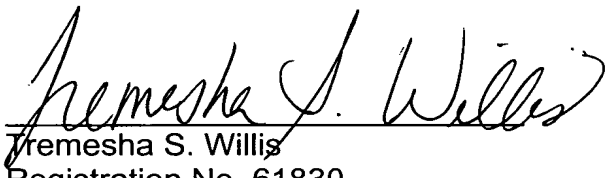
Accordingly, Applicant respectfully requests that the rejection to claims 1-15 under 35 U.S.C. §103(a) be withdrawn.

Conclusion

Based on at least the foregoing amendments and remarks, Applicant submits that claims 1-15 are allowable, and that this application is in condition for allowance. Accordingly, Applicant requests a favorable examination and consideration of the instant application. In the event the instant application can be placed in even better form, Applicant requests that the undersigned attorney be contacted at the number below.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: October 20, 2008 By: 

Tremesha S. Willis
Registration No. 61830

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620